

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT APPLICATION of :
Mistuhiko WATANABE :
Serial No.: [NEW] : Attn: Applications Branch
Filed: October 21, 2003 : Attorney Docket No.: OKI.592
For: MICROCOMPUTER AND TEST METHOD THEREFOR

CLAIM OF PRIORITY

Honorable Assistant Commissioner for Patents and Trademarks,
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant, in the above-identified application, hereby claims the priority date
under the International Convention of the following Japanese application:

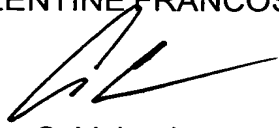
Appln. No. 2002-354726 filed December 6, 2002

as acknowledged in the Declaration of the subject application.

A certified copy of said application is being submitted herewith.

Respectfully submitted,

VOLENTINE FRANCOS, PLLC



Adam C. Volentine
Registration No. 33,289

12200 Sunrise Valley Drive, Suite 150
Reston, Virginia 20191
Tel. (703) 715-0870
Fax. (703) 715-0877

Date: October 21, 2003

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 2 年 1 2 月 6 日
Date of Application:

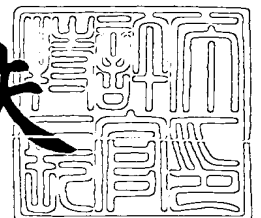
出 願 番 号 特 願 2 0 0 2 - 3 5 4 7 2 6
Application Number:
[ST. 10/C] : [J P 2 0 0 2 - 3 5 4 7 2 6]

出 願 人 沖 電 気 工 業 株 式 有 限 公 司
Applicant(s):

2 0 0 3 年 8 月 2 1 日

特 許 庁 長 官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願

【整理番号】 KA003842

【提出日】 平成14年12月 6日

【あて先】 特許庁長官 太田 信一郎 殿

【国際特許分類】 G01R 31/28
G06F 11/22

【発明者】

【住所又は居所】 東京都港区虎ノ門1丁目7番12号 沖電気工業株式会社
社内

【氏名】 渡辺 充博

【特許出願人】

【識別番号】 000000295

【氏名又は名称】 沖電気工業株式会社

【代理人】

【識別番号】 100086807

【弁理士】

【氏名又は名称】 柿本 恭成

【手数料の表示】

【予納台帳番号】 007412

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9001054

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 マイクロコンピュータとその試験方法

【特許請求の範囲】

【請求項 1】 通常動作用のプログラムが格納された第 1 のメモリと、
機能試験用のプログラムが格納された第 2 のメモリと、
外部端子から与えられる信号を監視して試験モードが指定されたことを検出する試験モード検出回路と、

前記試験モードが指定されていないときには前記第 1 のメモリにアクセスして前記通常動作用のプログラムを実行し、該試験モードが指定されたときには前記第 2 のメモリにアクセスして前記機能試験用のプログラムを実行する中央演算処理装置と、

前記第 1 及び第 2 のメモリに対するアクセスアドレス及びデータを監視し、許可されていない不正なアクセスがあったときに前記中央演算処理装置に対して特定の動作を実行させるメモリ管理ユニットと、

前記試験モード時に前記中央演算処理装置からセキュリティ試験信号が出力され、かつ特定のメモリ領域がアクセスされたときに、予め設定された特定の命令を該中央演算処理装置に与える試験回路とを、

備えたことを特徴とするマイクロコンピュータ。

【請求項 2】 前記試験回路から前記中央演算処理装置に与える特定の命令は、前記メモリ管理ユニットで不正なアクセスとして検出される命令であることを特徴とする請求項 1 記載のマイクロコンピュータ。

【請求項 3】 通常動作用のプログラムが格納された第 1 のメモリと、機能試験用のプログラムが格納された第 2 のメモリと、外部端子から与えられる信号を監視して試験モードが指定されたことを検出する試験モード検出回路と、前記試験モードが指定されていないときには前記第 1 のメモリにアクセスして前記通常動作用のプログラムを実行し、該試験モードが指定されたときには前記第 2 のメモリにアクセスして前記機能試験用のプログラムを実行する中央演算処理装置と、前記第 1 及び第 2 のメモリに対するアクセスアドレス及びデータを監視し、許可されていない不正なアクセスがあったときに前記中央演算処理装置に対して

特定の動作を実行させるメモリ管理ユニットとを備えたマイクロコンピュータにおいて、

前記中央処理装置は、前記機能試験用のプログラムによってセキュリティ試験が実行されており、かつ前記前記メモリ管理ユニットから前記特定の動作の実行が指示されたときに、所定の例外処理を行う例外処理回路を有することを特徴とするマイクロコンピュータ。

【請求項 4】 プログラムを格納するメモリと、前記メモリに格納されたプログラムを実行する中央演算処理装置と、前記メモリに対するアクセスを監視して不正なアクセスを検出したときに前記中央演算処理装置に対して割り込み信号を出力するメモリ管理ユニットとを有するマイクロコンピュータの試験方法であって、

前記メモリの第 1 のアドレスに第 2 のアドレスへの分岐命令を書き込む処理と、

前記メモリ管理ユニットに対して、前記第 2 のアドレスの実行を不正なアクセスとして設定する処理と、

前記第 1 のアドレスに分岐する処理と、

前記第 1 のアドレスに書き込まれた分岐命令の実行の結果、前記メモリ管理ユニットから前記割り込み信号が出力されたか否かによって故障の有無を判定する処理とを、

順次実行することを特徴とするマイクロコンピュータの試験方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、I C カードのようにセキュリティ機能を有するマイクロコンピュータ、特にそのセキュリティ機能を試験するための試験回路を備えたマイクロコンピュータとその試験方法に関するものである。

【0 0 0 2】

【従来の技術】

【0 0 0 3】

【特許文献 1】

特開平 0 6 - 3 2 4 9 7 2 号公報

【特許文献 2】

特開平 0 8 - 2 7 2 6 9 5 号公報

【0 0 0 4】

一般に L S I（大規模集積回路）は、シリコンウエハ上に微細な加工をしたりチップをパッケージに組み立てる製造過程において、ある確率で製造欠陥による動作不良品が発生する。従って、製造時に、出来上がった L S I に電源と信号を印加し、期待どおりの動作をするか否かの試験を行って不良品を除去する。このため、可制御性・可観測性を向上させる目的で、L S I の論理設計時にスキャン機能等の試験回路を予め組み込んでおく試験容易化設計が行われている。

【0 0 0 5】

ここで、可制御性とは、L S I 内部の任意の信号を任意のレベル（“H”または“L”）に設定できることであり、可観測性とは、この L S I 内部の任意の信号のレベルを検出できることである。すべての信号のレベルを L S I の外部に出力して直接検出することは不可能なので、スキャン機能では、内部信号のレベルの変化を特定の端子の出力パターンの変化として出力させるような構成が採用されている。

【0 0 0 6】

しかし、可制御性・可観測性を高くすることは、内部信号を制御・検出できるということであり、セキュリティに関連する L S I では、そのセキュリティのレベルを下げることになる。パスワードや秘密鍵のように他人に知られてはならないデータを読み出されてしまうおそれがあるからである。

【0 0 0 7】

特に、I C カード用のマイクロコンピュータでは、I S O 7 8 1 6 の規格で、端子形状と信号の電気的特性が規定され、外部接続用の端子は、電源（V D D、G N D）、クロック（C L K）、リセット（R S T）、及び半二重通信用の直列データ（S I O）の 5 端子のみに限定されている。このようなマイクロコンピュータは、セキュリティ用途であることと、外部接続用の端子数が少ないことから

、試験に関して種々の制約がある。

【0 0 0 8】

更に、外部からアプリケーション・プログラムをダウンロードして実行できる高機能なセキュリティ向けのマイクロコンピュータでは、不正なプログラムがダウンロードされてパスワードや秘密鍵のデータを読み書きするような処理から保護するために、アプリケーション・プログラムにおける特定命令の実行や、特定領域へのアクセス及び分岐等を禁止するような高度のセキュリティ機能が必要である。

【0 0 0 9】

図 2 は、上記の機能を備えた従来のマイクロコンピュータの一例を示す構成図である。

【0 0 1 0】

このマイクロコンピュータは、CPU（中央演算処理装置）1、ROM（不揮発性メモリ）2、3、RAM（随時読み書き可能メモリ）4、周辺回路 5、バス（またはブリッジ）6、セキュリティ回路 7、試験用回路 8、及び試験モード検出回路 9 を備えている。

【0 0 1 1】

CPU 1 は、ROM 2、3 等のメモリに格納された命令を逐次実行するものである。ROM 2 は、このマイクロコンピュータの主要な動作を決める OS（オペレーティング・システム）等のプログラムを格納したメモリである。ROM 3 は、チップの製造試験用のプログラム、セキュリティ用の最小限のライブラリ、ファンクションコール用のサブルーチン等を格納したメモリである。

【0 0 1 2】

RAM 4 は、データを格納したりプログラムを一時的に格納するためのメモリで、電氣的に書き換え可能な不揮発性メモリも含まれる。周辺回路 5 は、暗号処理や外部との通信を行うための回路である。バス 6 は、CPU 1 とその他の ROM 2、3 等の回路との接続部分で、トライステートバスや OR バスといったバス接続やブロック間の論理やタイミングを調整するブリッジ回路が用いられる。

【0 0 1 3】

セキュリティ回路 7 は、C P U 1 が読み出したアドレスや命令を逐次監視し、実行や読み書きが許可されていないプログラム領域やデータ領域へのアクセスがあった場合に、C P U 1 に対して不正アクセク検出信号 I L を出力して、適切な処理を行わせるための回路である。

【 0 0 1 4 】

試験用回路 8 は、チップ上に設けられて外部には接続されていない複数の試験信号入力端子 8 a と、試験モード信号 T M で切り替え制御されるセクタ 8 b を有している。試験用回路 8 は、製造試験時に試験装置のプローブを介して試験信号入力端子 8 a から C P U 1 に試験用の命令を与え、任意の命令系列を実行させて、アプリケーション・プログラムを正しく実行できるか否か、或いは周辺回路 5 が正しく動作するか否かを試験する回路である。

【 0 0 1 5 】

試験モード検出回路 9 は、端子 C L K, R S T, S I O に与えられる特定シーケンスの信号パターンを検出して、このマイクロコンピュータが試験モードに設定されたことを示すために、試験用回路 8 に対する試験モード信号 T M をアクティブにするものである。

【 0 0 1 6 】

次に動作を説明する。

【 0 0 1 7 】

このようなマイクロコンピュータにおいて製造時に行われる試験動作では、端子 C L K, R S T, S I O に試験モードを設定するための特定の信号パターンが与えられる。これにより、試験モード検出回路 9 から出力される試験モード信号 T M がアクティブにされ、試験用回路 8 の試験信号入力端子 8 a が C P U 1 に接続される。更に、外部の試験装置から試験信号入力端子 8 a に試験用の命令を与え、C P U 1 に任意の命令系列を実行させてユーザアプリケーションを正しく実行できるか否か、或いは周辺回路 5 が正しく動作するか否かを試験する。

【 0 0 1 8 】

一方、通常動作時には、C P U 1 から出力されたアドレス A D R は、セキュリティ回路 7 によって常に監視され、アクセスが許可された領域内か否かの判別が

行われる。実行が許可された領域であれば、ROM 2, 3 等のメモリから読み出された命令は、CPU 1 によってそのまま実行される。実行が禁止された領域であれば、セキュリティ回路 7 から不正アクセス検出信号 IL が出力され、CPU 1 によってプログラムの実行の中断や、アクセスの無効化等の処理が行われる。

【0 0 1 9】

【発明が解決しようとする課題】

しかしながら、従来のマイクロコンピュータでは、次のような課題があった。

【0 0 2 0】

(a) 試験用回路 8 は、外部の試験装置から試験用の命令を与えるための試験信号入力端子 8 a を有している。この試験信号入力端子 8 a は、外部の入出力ピンには接続されていないが、チップ上に試験用のパッドとして形成されているため、悪意ある第 3 者によって、そのパッドを介してデータを読み出したり、不正なプログラムをダウンロードする等のセキュリティの侵害が行われる危険性がある。

【0 0 2 1】

(b) 不正アクセス検出信号 IL の配線パターンが電源の GND や VDD とショートしていたり、セキュリティ回路 7 からこの不正アクセス検出信号 IL を出力するトランジスタの動作不良で、不正アクセス検出信号 IL が正しく出力されていないことを検出することができない。この理由は、次のとおりである。

【0 0 2 2】

ROM 3 に格納した試験プログラムに基づいて CPU 1 がセキュリティ機能を自己試験し、不良の有無を端子 CLK, RST, SIO から出力する必要がある。これには、例えば RAM 4 に格納されたユーザアプリケーションによって、例外状態（不正な命令実行を検出した状態）を起こさせてそれが検出できるか、及び適正な動作時に例外状態が発生しないかを、分岐先のプログラムを実行することなく、試験用プログラムの実行の流れや読み出しデータの変化として、CPU 1 で検出しなければならない。ここで、分岐先プログラムを実行することができないのは、ROM 2 には OS が格納されており、どのアドレスにどの命令が格納されているかを特定できないため、もし実行するとその後の CPU 1 の動作も特

定できず、試験用プログラムへ復帰することができないからである。従って、このような処理を行うことは、図 2 のマイクロコンピュータの構成では不可能であった。

【 0 0 2 3 】

【課題を解決するための手段】

前記課題を解決するために、本発明は、セキュリティ機能を有するマイクロコンピュータを、通常動作用のプログラムが格納された第 1 のメモリと、機能試験用のプログラムが格納された第 2 のメモリと、外部端子から与えられる信号を監視して試験モードが指定されたことを検出する試験モード検出回路と、前記試験モードが指定されていないときには前記第 1 のメモリにアクセスして前記通常動作用のプログラムを実行し、該試験モードが指定されたときには前記第 2 のメモリにアクセスして前記機能試験用のプログラムを実行する CPU と、前記第 1 及び第 2 のメモリに対するアクセスアドレス及びデータを監視し、許可されていない不正なアクセスがあったときに前記 CPU に対して特定の動作を実行させるメモリ管理ユニットと、前記試験モード時に前記 CPU からセキュリティ試験信号が出力され、かつ特定のメモリ領域がアクセスされたときに、予め設定された特定の命令を該 CPU に与える試験回路とで構成している。

【 0 0 2 4 】

本発明によれば、以上のようにマイクロコンピュータを構成したので、機能試験において次のような作用が行われる。

【 0 0 2 5 】

外部端子の信号で試験モードが入力されて試験モード検出回路で検出されると、CPU によって第 2 のメモリのプログラムが読み出され、機能試験が実行される。機能試験の中で、セキュリティ試験信号が出力され、更に特定のメモリ領域がアクセスされると、試験回路から予め設定された特定の命令が CPU に与えられる。従って、例えば、この特定の命令を不正なアクセスを行うような命令にしておけば、その命令を実行した時点でメモリ管理ユニットから CPU に特定の動作をさせるような制御が行われるはずである。もしも、特定の動作が行われなければ、メモリ管理ユニットが故障していることが判明する。

【 0 0 2 6 】**【発明の実施の形態】**

図 1 は、本発明の実施形態を示すマイクロコンピュータの構成図であり、図 2 中の要素と共通の要素には共通の符号が付されている。

【 0 0 2 7 】

このマイクロコンピュータは、セキュリティ機能を有するもので、図 2 と同様の CPU 1、ROM 2、3、RAM 4、周辺回路 5、バス（またはブリッジ） 6、セキュリティ回路 7、及び試験モード検出回路 9 と、図 2 とは異なる試験用回路 10 を備えている。

【 0 0 2 8 】

CPU 1 は、ROM 2、3 等のメモリに格納された命令を逐次実行するものである。ROM 2 は、このマイクロコンピュータの主要な動作を決める OS 等のプログラムを格納した読み出し専用のメモリであり、ROM 3 は、チップの製造試験用のプログラム、セキュリティ用の最小限のライブラリ、ファンクションコール用のサブルーチン等を格納した読み出し専用のメモリである。

【 0 0 2 9 】

RAM 4 は、データを格納したりプログラムを一時的に格納するためのメモリで、電氣的に書き換え可能な不揮発性メモリも含まれる。周辺回路 5 は、暗号処理や外部との通信を行うための回路である。バス 6 は、CPU 1 とその他の ROM 2、3 等との接続部分で、トライステートバスや OR バスといったバス接続やブロック間の論理やタイミングを調整するブリッジ回路が用いられる。

【 0 0 3 0 】

セキュリティ回路 7 は、メモリ管理ユニットとも呼ばれ、CPU 1 が読み出したアドレスや命令を逐次監視し、実行や読み書きが許可されていないプログラム領域やデータ領域へのアクセスがあった場合に、CPU 1 に対して不正アクセス検出信号 IL を出力して、適切な処理を行わせるための回路である。

【 0 0 3 1 】

試験モード検出回路 9 は、端子 CLK、RST、SIO から与えられる特定シーケンスの信号パターンによって、LSI が試験モードに設定されたことを検出

し、CPU1 に対する試験モード信号 TM をアクティブにするものである。通常の動作中に誤って試験モードに移行することがないように、端子 CLK, RST, SIO には、通常の動作では起こり得ない信号パターンを与えるようにしている。例えば、リセット (RES = "L") 期間中に、端子 CLK のクロックに同期して特定の信号パターンを端子 SIO に与え、LSI のプログラムでその信号パターンを識別して試験状態に移行するような方法が採用されている。

【0032】

試験用回路 10 は、製造試験時に CPU1 に試験用の命令を実行させ、アプリケーション・プログラムを正しく実行できるか否か、周辺回路 5 が正しく動作するか否か等を試験するための回路である。

【0033】

この試験用回路 10 は、レジスタ 11、セクタ 12、アドレスデコーダ 13、及び AND (論理積ゲート) 14 を有している。レジスタ 11 は、特定の命令コードを格納するものであり、セクタ 12 は、メモリ 2～4 から読み出されてバス 6 を介して出力された読み出しデータ RDT とレジスタ 11 に格納された特定の命令を選択して CPU1 に出力するものである。

【0034】

アドレスデコーダ 13 は、バス 6 から出力されるアドレス ADR を解読して、ROM 2 が選択されたときにその出力信号をアクティブにするものである。AND 14 は、CPU1 から与えられるセキュリティ試験信号 ST とアドレスデコーダ 13 の出力信号が共にアクティブになったときに、セクタ 11 をレジスタ 12 側に切り替えるための切替信号を出力するものである。

【0035】

図 3 及び図 4 は、図 1 の動作を示すフローチャート (その 1、及びその 2) である。以下、これらの図 3 及び図 4 を参照しつつ、図 1 の試験時の動作を説明する。

【0036】

図 3 には、RAM 4 に格納されたアプリケーション・プログラムから、分岐を禁止した ROM 2 上の領域へ分岐した際に、この ROM 2 上での命令実行を許可

してしまう故障の有無を試験するプログラムの処理手順が示されている。ここでは、アプリケーション・プログラムが格納された R A M 4 のアドレス A P P から、O S が格納された R O M 2 のアドレス S Y S への分岐を許可した場合を想定している。

【 0 0 3 7 】

まず、端子 C L K, R S T, S I O に、試験モードを設定するための信号パターンを印加する。これにより、試験モード検出回路 9 から出力される試験モード信号 T M がアクティブとなり、C P U 1 によって R O M 3 に格納された試験プログラムの実行が開始される。

【 0 0 3 8 】

図 3 のステップ S 1 において、C P U 1 から出力されるセキュリティ試験信号 S T をアクティブにする。

【 0 0 3 9 】

ステップ S 2 において、R A M 4 のアプリケーション・プログラム内のアドレス A P P に、O S 内のアドレス S Y S への分岐命令の命令コードを書き込む。これにより、C P U 1 がアドレス A P P の命令を実行すると、アプリケーション・プログラムから O S への分岐処理が実現できるようになる。

【 0 0 4 0 】

ステップ S 3 において、アプリケーション・プログラム内のアドレス A P P でのプログラムの実行を禁止するように、セキュリティ回路 7 を設定する。

【 0 0 4 1 】

ステップ S 4 において、スタックに試験プログラム中の故障判定ルーチン 1 の先頭アドレス J D G 1 をプッシュする。

【 0 0 4 2 】

ステップ S 5 において、アドレス A P P へ分岐する。具体的には、試験プログラムからアドレス A P P への分岐命令を実行する。これにより、C P U 1 のプログラム・カウンタに値 A P P が転送され、次の命令フェッチはアドレス A P P から行われる。

【 0 0 4 3 】

ステップS6において、アドレスAPPにはOS内のアドレスSYSへの分岐命令が格納されているので、CPU1は続いてアドレスSYSへの分岐命令を実行する。アドレスSYSの命令フェッチが検出されると、試験用回路10中のセレクタ12は、レジスタ11側に切り替えられる。これにより、レジスタ11に格納されている特定の命令、例えばサブルーチン復帰命令がCPU1へ与えられる。CPU1は、そのサブルーチン復帰命令をフェッチし、そのフェッチしたサブルーチン復帰命令を実行する。

【0044】

ステップS7では、サブルーチン復帰命令の実行結果による例外状態の発生の有無が判定される。もしも、セキュリティ回路7またはその出力系統に故障があると、例外状態が発生しないのでステップS8へ進む。また、セキュリティ回路7が正常に動作していれば、例外状態が発生してステップS9へ進む。

【0045】

ステップS8では、セキュリティ回路7の故障のために例外状態が発生しないので、サブルーチン復帰命令が実行され、スタックに格納された故障判定ルーチンJDG1がポップされてCPU1の命令実行が移行する。ステップS8の後、ステップS10へ進む。

【0046】

一方、ステップS9では、正常な動作として例外条件が発生し、予め定められた例外処理ルーチンへ分岐する。例外処理ルーチンでは、割り込みフラグを立てて例外状態の発生を記憶し、この例外処理ルーチンからの復帰命令を実行する。ステップS9の後、ステップS10へ進む。

【0047】

ステップS10において、スタックには故障判定ルーチン1の先頭アドレスJDG1が格納されているので、CPU1の命令実行は、この故障判定ルーチン1へ分岐する。

【0048】

ステップS11において、故障判定ルーチン1は、割り込みフラグの状態に応じて、故障の有無の判定結果を端子SIOを通して外部に出力する。即ち、割り

込みフラグが立っていれば故障がない旨の信号を出力し、割り込みフラグが立っていないければ故障がある旨の信号を出力する。これにより、セキュリティ回路 7 の故障の有無を知ることができる。

【 0 0 4 9 】

図 4 には、R A M 4 に格納されたアプリケーション・プログラムから、分岐を許可した R O M 2 上の領域へ分岐した際に、R O M 2 上での命令実行を禁止してしまう故障の有無を試験するプログラムの処理手順が示されている。ここでは、図 3 と同様に、アプリケーション・プログラムが格納された R A M 4 のアドレス A P P から、O S が格納された R O M 2 のアドレス S Y S への分岐を許可した場合を想定しており、この図 3 中のステップと処理内容が同一のステップには、同一の符号が付されている。

【 0 0 5 0 】

図 4 の処理では、図 3 中のステップ S 3 , S 4 , S 7 ~ S 1 1 に代えて、それぞれ若干処理内容の異なるステップ S 3 A , S 4 A , S 7 A ~ S 1 1 A を有している。

【 0 0 5 1 】

ステップ S 3 A では、アプリケーション・プログラム内のアドレス A P P でのプログラムの実行を許可するように、セキュリティ回路 7 を設定する。

【 0 0 5 2 】

ステップ S 4 A では、スタックに試験プログラム中の故障判定ルーチン 2 の先頭アドレス J D G 2 をプッシュする。

【 0 0 5 3 】

ステップ S 7 A では、サブルーチン復帰命令の実行結果による例外状態の発生の有無が判定される。セキュリティ回路 7 が正常に動作していれば、例外状態が発生しないのでステップ S 8 A へ進む。もしも、セキュリティ回路 7 またはその出力系統に故障があれば、例外状態が発生してステップ S 9 A へ進む。

【 0 0 5 4 】

ステップ S 8 A では、正常な動作として例外状態が発生しないので、サブルーチン復帰命令が実行され、スタックに格納された故障判定ルーチン J D G 2 がポ

ップされてCPU1の命令実行が移行する。ステップS8Aの後、ステップS10Aへ進む。

【0055】

一方、ステップS9Aでは、故障のために例外状態が発生し、予め定められた例外処理ルーチンへ分岐する。例外処理ルーチンでは、割り込みフラグを立てて例外状態の発生を記憶し、この例外処理ルーチンからの復帰命令を実行する。ステップS9Aの後、ステップS10Aへ進む。

【0056】

ステップS10Aにおいて、スタックには故障判定ルーチン2の先頭アドレスJDG2が格納されているので、CPU1の命令実行は、この故障判定ルーチン2へ分岐する。

【0057】

ステップS11Aにおいて、故障判定ルーチン2は、割り込みフラグの状態に応じて、故障の有無の判定結果を端子SIOを通して外部に出力する。即ち、割り込みフラグが立っていれば故障がある旨の信号を出力し、割り込みフラグが立っていなければ故障がない旨の信号を出力する。その他の処理は、図3と同様である。

【0058】

このように、本実施形態のマイクロコンピュータは、次のような利点がある。

【0059】

(1) 端子CLK, RST, SIO, VDD, GND以外に、試験のための外部接続用端子や、チップ上の試験用パッドを必要としないので、悪意ある第3者によって、セキュリティの侵害が行われる危険性が少ない。

【0060】

(2) 故障の有無で分岐先アドレスが異なるように構成しているので、セキュリティ回路7の試験を、不正アクセス検出信号ILが“L”に固定された場合と、“H”に固定された場合の2通りの故障モードに対して行うことができる。

【0061】

(3) (2)の試験において、ROM2上にあるOS内部のプログラムを実行

することなく、RAM 4 上にあるアプリケーション・プログラムの領域から ROM 2 への分岐の許可／禁止の試験ができる。従って、OS の内容を知らなくても試験用のプログラムを作成することができる。

【0062】

(4) CPU 1 やメモリ 2 ～ 4 は、従来どおりのものを用いることができるので、この発明を実施するために、既存の回路を変更する工数を最小限に抑えることができる。

【0063】

なお、本発明は、上記実施形態に限定されず、種々の変形が可能である。

【0064】

図 5 (a) ～ (d) は、図 1 のマイクロコンピュータの変形例を示す図であり、いずれも上記実施形態と同様の利点を有している。

【0065】

図 5 (a) のマイクロコンピュータは、バスと CPU の間に試験用回路を設けるのではなく、メモリ (ROM) の内部にセキュリティ回路の試験のためのセレクトを設け、通常動作時にはこのメモリから読み出されたデータを出力し、セキュリティ試験が指定されたときにはレジスタに格納された特定の命令を出力するように構成している。

【0066】

図 5 (b) のマイクロコンピュータは、CPU の内部に例外処理回路を設け、セキュリティ試験が指定され、かつ試験対象のメモリが選択されている時に、セキュリティ回路が不正アクセスを検出した場合に、例外状態を発生させるか特殊な動作モードへの移行を行うようにしている。

【0067】

図 5 (c) のマイクロコンピュータは、セキュリティ試験が指定され、かつ試験対象のメモリが選択されている時に、このメモリから読み出された命令のビットパターンに対し、“1” にしたいビットを OR ゲートによって、“0” にしたいビットを AND ゲートによって、置換を実現するものである。この回路では、通常動作時には、メモリから読み出されたデータが、AND や OR を介してその

まま CPU に与えられるようになっている。

【0 0 6 8】

図 5 (d) のマイクロコンピュータは、セキュリティ試験が指定されたときに、メモリに対する制御信号がアクティブになることを禁止すると共に、トライステートバッファを用いて、レジスタからバスに特定の命令コードを出力するように構成している。

【0 0 6 9】

【発明の効果】

以上詳細に説明したように、本発明によれば、試験モード時に CPU からセキュリティ試験信号が出力され、かつ特定のメモリ領域がアクセスされたときに、予め設定された特定の命令をこの CPU に与える試験回路を有している。従って、第 2 のメモリに機能試験用のプログラムを予め格納しておくことで所定の機能試験が可能になり、試験用のパッドを設ける必要がなくなってセキュリティが向上する。更に、特定の命令として不正なアクセスを起こさせるような命令を設定しておけば、メモリ管理ユニットの動作確認も可能になるという効果がある。

【図面の簡単な説明】

【図 1】

本発明の実施形態を示すマイクロコンピュータの構成図である。

【図 2】

従来のマイクロコンピュータの一例を示す構成図である。

【図 3】

図 1 の動作を示すフローチャート（その 1）である。

【図 4】

図 1 の動作を示すフローチャート（その 2）である。

【図 5】

図 1 のマイクロコンピュータの変形例を示す図である。

【符号の説明】

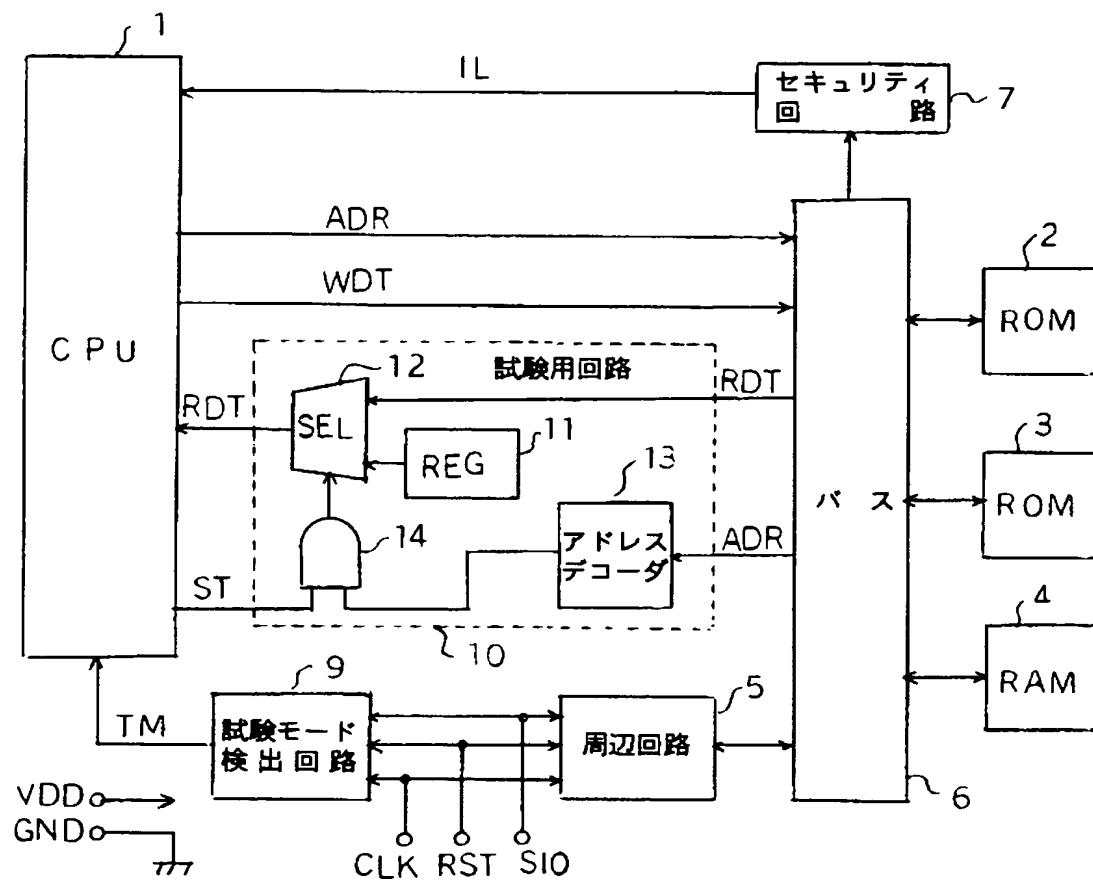
1 CPU

2, 3 ROM

- 4 R A M
- 5 周辺回路
- 6 バス
- 7 セキュリティ回路
- 9 試験モード検出回路
- 1 0 試験用回路
- 1 1 レジスタ
- 1 2 セレクタ
- 1 3 アドレスデコーダ
- 1 4 A N D

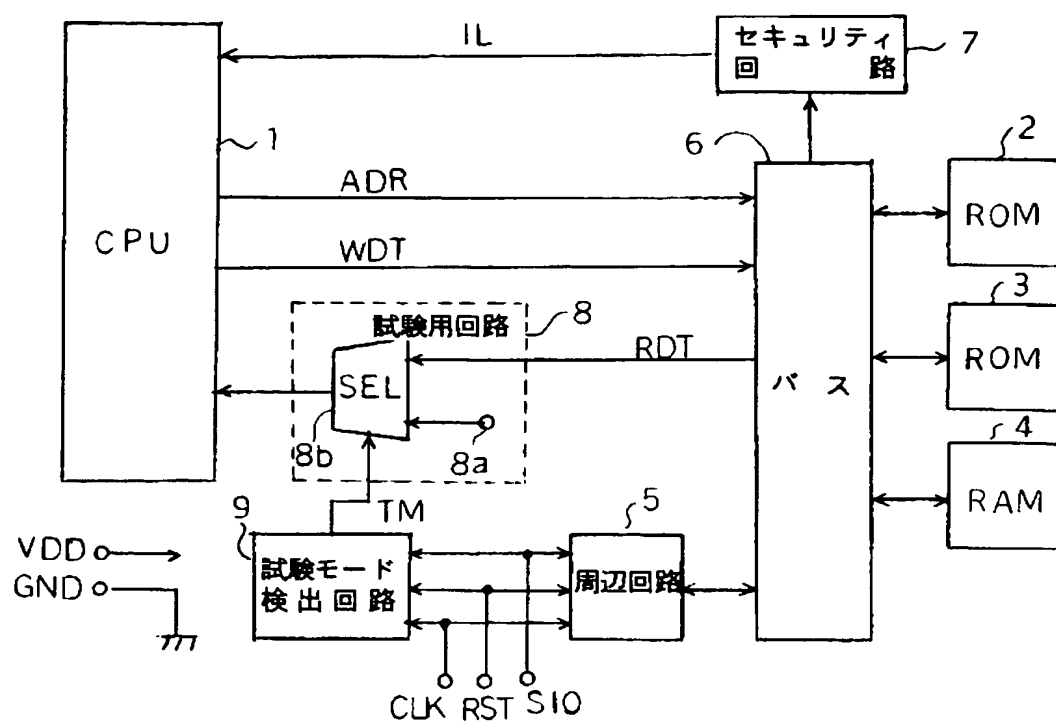
【書類名】 図面

【図 1】



本発明の実施形態のマイクロコンピュータ

【図 2】



従来のマイクロコンピュータ

【図 3】

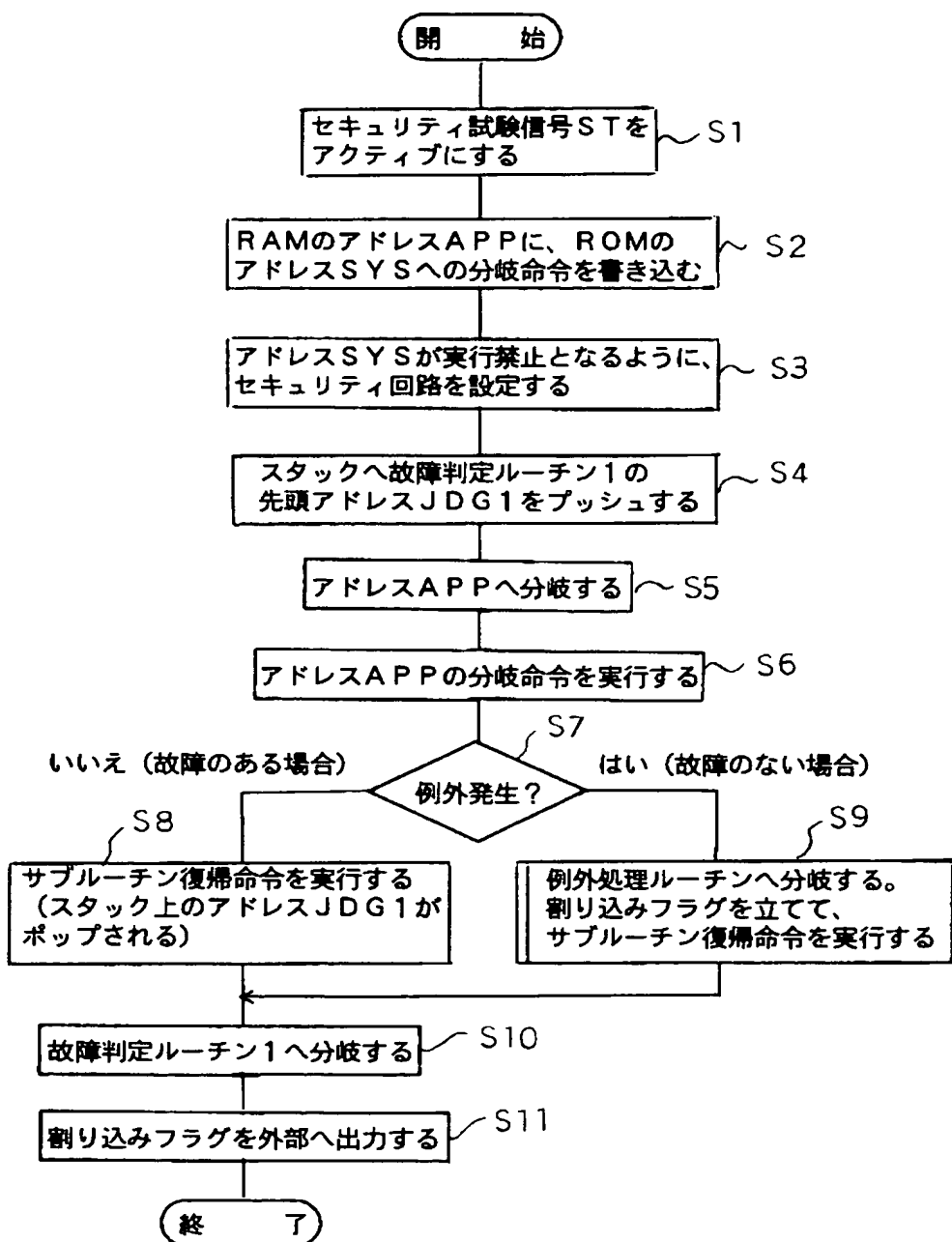


図 1 の動作 (その 1)

【図 4】

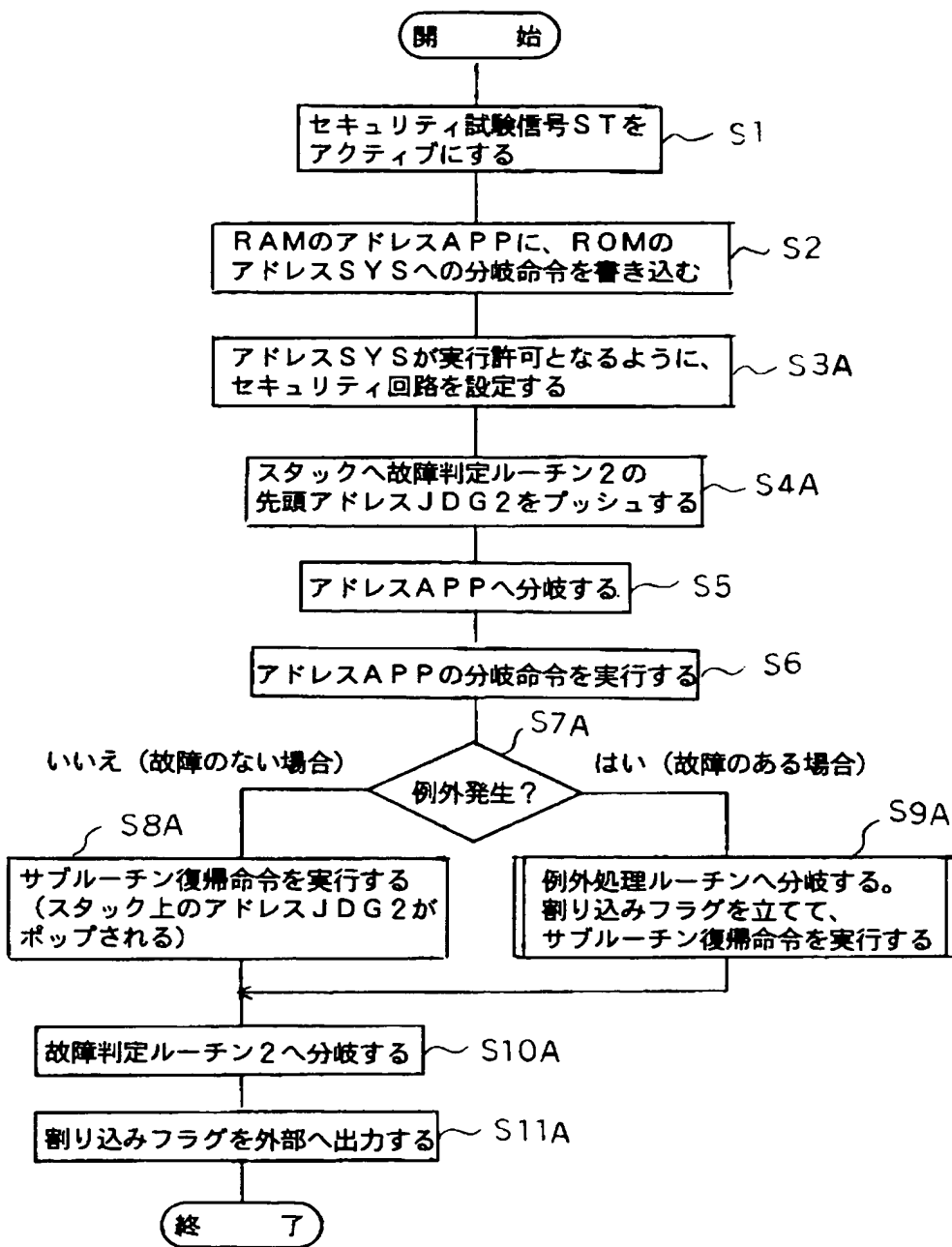


図 1 の動作 (その 2)

【図 5】

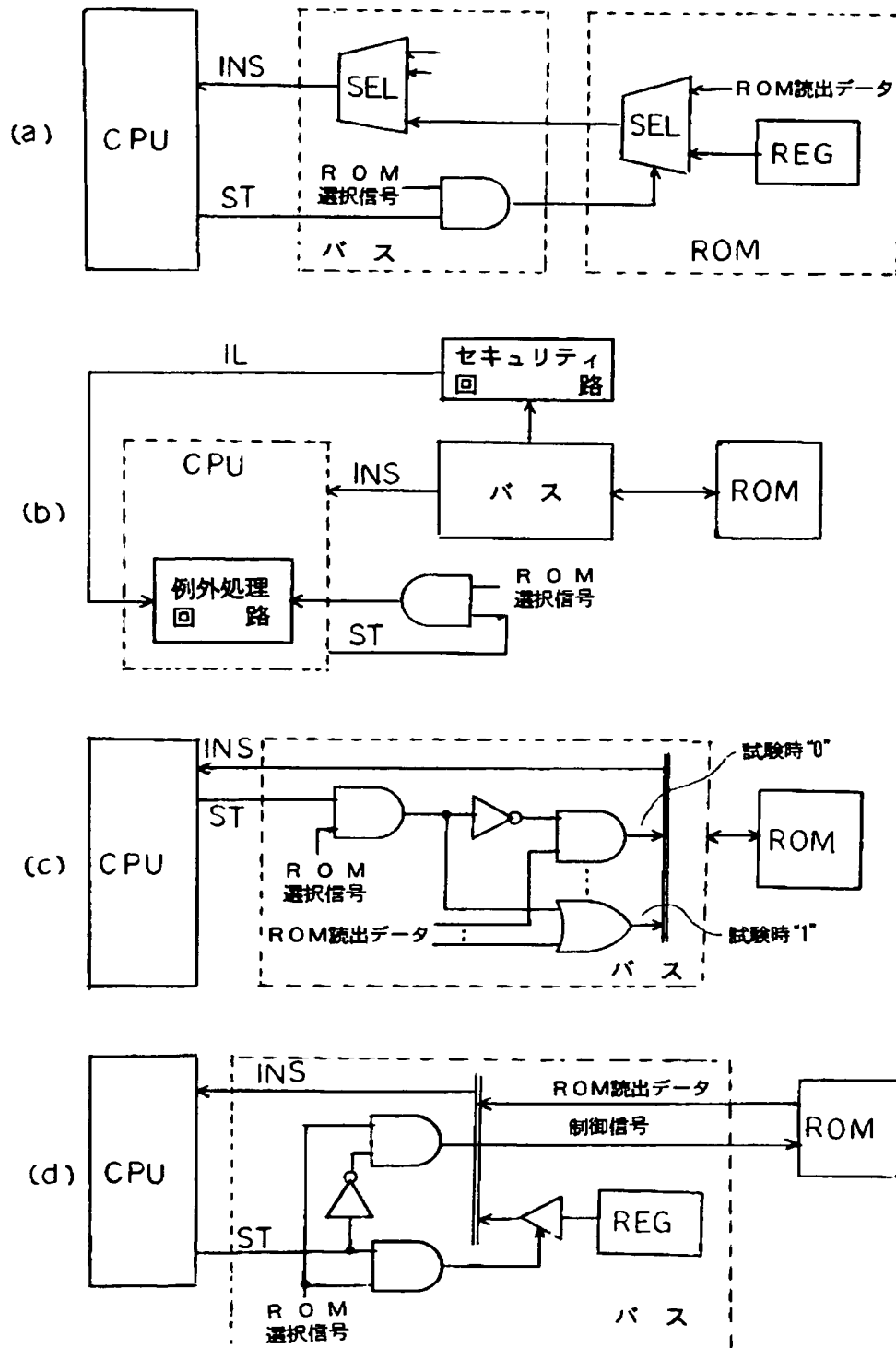


図 1 のマイクロコンピュータの変形例

【書類名】 要約書

【要約】

【課題】 チップ上に試験用のパッドを設けずに、セキュリティ回路の機能を含む各種の自己試験ができるマイクロコンピュータを提供する。

【解決手段】 外部端子CLK, RST, SIOから与えられる信号で試験モード信号TMがアクティブにされると、CPU1によってROM3に格納された各種の自己試験プログラムが読み出されて実行される。試験プログラムでセキュリティ回路7の試験になると、セキュリティ試験信号STがアクティブとなり、更に所定のアドレスADRがアクセスされると、試験用回路10のAND14の出力信号によってセクタ12がレジスタ11側に切り替えられる。レジスタ11には、例えば不正命令が設定されており、この不正命令がCPU1に与えられる。CPU1が不正命令を実行した時に、不正アクセス検出信号ILが出力されるか否かによってセキュリティ回路7の良否を判別する。

【選択図】 図1

特願 2 0 0 2 - 3 5 4 7 2 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 0 2 9 5]

1. 変更年月日

1 9 9 0 年 8 月 2 2 日

[変更理由]

新規登録

住 所

東京都港区虎ノ門1丁目7番12号

氏 名

沖電気工業株式会社